

MEMORANDUM

TO: OIG Staff
 Navarro and Oppenheim Contractors
 FDC Contractors

FROM: E. R. Quatrevaux
 Inspector General

DATE: February 29, 2000

SUBJ: Assessment of 1999 Case Statistical Data--Screening Directive

The *Assessment of 1999 Case Statistical Data* is a project mandated by Congress to be conducted by the Office of Inspector General (OIG). As Congress directed in the FY2000 Appropriation for the Legal Services Corporation (LSC), "[t]he Office of Inspector General will assess the case service information provided by the grantees, and will report to the Committee no later than July 30, 2000, as to its accuracy" (H.R. Report 106-283, p. 130).

In order to complete this assessment, the OIG will call on a sample of grantees to submit to the OIG specified data elements supporting their case reporting to LSC. This sampling plan is complemented by a carefully designed approach to the collection, maintenance and use of data submitted by selected grantees. This latter approach is informed by the OIG's desire to allay grantees' concerns regarding attorney-client privilege (i.e., no disclosure of privileged information to a third party) while helping the OIG to complete its report on the accuracy of case statistical data. Based on the assumption that some grantees may consider disclosure of the combination of client name and legal problem code (as such terms are defined in LSC's *CSR Handbook*) to infringe attorney-client privilege, the OIG will implement a screening procedure similar to a so-called "Chinese

wall”¹ to keep legal problem code completely separate from the case’s associated client name.²

In the first phase of data collection, a sample of grantees will be required to submit eight to ten data elements, including legal problem codes but not including client names (Codes Data). The second phase of data collection will require a sample of grantees (some of which will be in the Codes Data sample) to submit a set of data elements, including client names but not including legal problem codes (Names Data). The OIG will use these data as part of its assessment of case statistical data accuracy.

The Inspector General hereby directs that the OIG’s collection, maintenance and use of data be in accordance with procedures that ensure the complete segregation of client names from associated legal problem codes such that any OIG personnel (which shall include OIG staff and contractors) with access to a client name shall not gain access to the associated legal problem code, and any personnel with access to a legal problem code shall not gain access to the associated client name. ***The Inspector General hereby directs*** that the following procedures be implemented:

- (1) Codes Data received and/or maintained in electronic format shall be maintained by the Codes Data Team. Passwords shall be necessary to access Codes Data on electronic hardware. Passwords shall be known only to the Codes Data Team.
- (2) Hard (paper) copies³ of Codes Data shall be maintained by the Codes Data Team and when not in use, shall be kept in a locked safe, accessible only to the Codes Data Team.
- (3) Names Data received and/or maintained in electronic format shall be maintained by a team of OIG personnel (Names Data Team) separate from any OIG personnel with access to Codes Data (Codes Data

¹ More generally, a “Chinese wall” is used to prevent the perception that an “insulated area of a firm or company has in fact used or will be in the position to use confidential information possessed by another part of the same firm or company.” (Aitken, L. (1992) Chinese Walls and Conflicts of Interest, 18 Monash University Law Review, 91, 93.) The procedures for implementing the wall within the OIG have been adapted from *Cromley v. Board of Education*, 17 F3d 1059 (7th Cir. 1994).

² The OIG recognizes that only a limited subset of problem codes have the potential for impinging on attorney-client privilege, however, the data collection plan has been designed to prevent any such concatenation, whether such a concatenation would appear to be privileged or not.

³ This includes data received in hard copy or received in electronic format and later converted to hard copy.

- Team). Electronic Names Data will not be maintained on the OIG network, but will be maintained on a separate notebook computer. A password shall be necessary to access Names Data on electronic hardware. This password shall be known only to the Names Data Team. The Codes Data Team and the Names Data Team shall not share personnel.
- (4) Hard (paper) copies⁴ of Names Data shall be maintained by the Names Data Team and when not in use, shall be kept in a locked safe, accessible only to the Names Data Team. The notebook computer on which electronic Names Data is maintained also shall be kept in this locked file cabinet when not in use.
 - (5) As soon as practical, client names maintained in Names Data shall be deleted.
 - (6) The Names Data Team is prohibited from discussing or otherwise sharing the specific client names maintained in Names Data with the Codes Data Team, any other OIG personnel, or any other person. In addition, the Names Data Team shall take any and all precautions reasonably necessary to avoid the inadvertent disclosure of client names.
 - (7) The Codes Data Team is prohibited from discussing or otherwise sharing the specific legal problem codes maintained in Codes Data with the Names Data Team. In addition, the Codes Data Team shall take any and all precautions reasonably necessary to avoid the inadvertent disclosure of legal problem codes to the Names Data Team. The Codes Data Team may discuss or share Codes Data with OIG personnel not designated as a member of the Names Data Team on a need to know basis. Any OIG personnel receiving Codes Data, *e.g.*, in reports and/or spreadsheets, shall be subject to all restrictions on the Codes Data Team, *see especially*, the restrictions in paragraphs 2 and 7.
 - (8) OIG Personnel not designated as a member of the Names Data Team shall not discuss with any member of the Names Data Team specific client names in Names Data and shall not in any way attempt to access such client names.

⁴ See note 3.

- (9) This directive does not prohibit the sharing of data or other information when the sharing of same does not allow the linking of client names and associated legal problem codes.
- (10) Any OIG employee who intentionally violates any of the terms listed in paragraph (1) through (8) shall be subject to immediate termination of employment. In addition, on completion of the OIG Assessment of 1999 Case Statistical Data, the members of the Codes Data Team and the Names Data Team shall be required to attest, under oath, to their adherence to the procedures directed hereby.